State of Indiana Policy and Standards

Cloud Product and Service Agreements

Standard ID
IOT-CS-SEC-010

Published Date
10/3/2016

Effective Date
10/3/2016

Last Updated
9/28/2016

Next Review Date
9/28/2017

Policy
02.0 Business Environment (ID.BE)

02.1 ID.BE-1

02.1.1 Third-Party Governance

Purpose
Define the security requirements that a cloud provider must have in place before IOT will permit the State to enter into a cloud product or service agreement.

Scope
IOT Supported Entities

Statement
The State of Indiana prefers to host solutions/systems within the Indiana Office of Technology's (IOT) datacenters. In the event that a cloud provider offering Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) that IOT is unable to offer, agencies shall work with IOT as part of any procurement effort related to cloud service providers and/or offerings.

All direct IaaS solutions must be brokered through IOT using a blanket or pre-negotiated agreement, where the provider meets the following requirements:

- Systems must be Federal Risk and Authorization Management Program (FedRAMP) Authorized with the commensurate Federal Information Processing Standard (FIPS) 199 'High' baseline.
- Meet IOT's cloud hosting contractual agreement
- Meet or exceed IOT's State Policy and Standards
- Meet participating agencies' federal and state compliance regulations (e.g., Pub 1075, MARS-E 2.0)
- System Security Plan shall be created and updated annually based on the National Institute of Technology and Standards (NIST) Special Publication 800-53 (Revision 4) Controls
- Hosted solution can securely interconnect with existing systems within IOT's datacenter (if applicable)
- Data must reside, traverse and be supported only within the continental U.S

All PaaS or SaaS solutions where non-public data is collected, processed, transmitted, stored, or interconnected with a system that contains such data, shall be hosted on premise (IOT data centers) or meet the above requirements, where the acceptable FedRAMP Authorization is at a FIPS 'Moderate' level or higher. If the solution isn't hosted in a FedRAMP Authorized data center with the stated requirements, an exception must be granted by the State CIO. If an exception is granted, all other requirements other than FedRAMP are still applicable, with the following additional requirement:

- An annual third party data center security assessment must be completed by a reputable party and a report shall be provided to the State (e.g., SSAE16 SOC 2)

All cloud contracts shall use the State of Indiana boilerplate language for the service type (e.g., SaaS) and follow the appropriate procurement methods.

Roles

Agency Executive Management

Information Asset Owners/System Owners

IOT Personnel

Responsibilities

Information System Owners and Agency Management/Executive Management must follow the appropriate process related to procurement of cloud product and services. IOT shall broker all infrastructure cloud hosting services within the State's control and be involved in decision making for PaaS and SaaS solutions.

Management Commitment

Management shall ensure that appropriate processes and approvals take place prior to contracting with a cloud provider.

Coordination Among Organizational Entities

Agencies shall partner and communicate with IOT on any/all cloud product and service offerings.

Compliance

IOT may audit for validation of the requirements within this standard at any time. Agencies found out of compliance with this standard shall be escalated to the State CIO.

Exceptions

Exceptions must be formally approved by the State of Indiana CIO.